The Landscape of Electronic Data Safes and their Adoption in E-Government and E-Business

Pfister, Joachim ; Schwabe, Gerhard

Abstract: This article reports on the concept of electronic data safes for managing personal data and describes the landscape of existing services. Using an exploratory research approach, a model of hierarchical service layers is developed. It serves as a structure for orientation in this emerging field of tools and services. Furthermore, we identify factors and areas of interest that are relevant for the adoption of electronic data safes in e-government and e-business using the Unified Theory of Acceptance and Use of Technology as a theoretical lens. We conclude that clearly perceivable benefits are key facilitators for the adoption of electronic data safes by end-users.

DOI: https://doi.org/10.1109/HICSS.2013.532

The Landscape of Electronic Data Safes and their Adoption in E-Government and E-Business

Joachim Pfister
University of Zurich
pfister@ifi.uzh.ch

Gerhard Schwabe
University of Zurich
schwabe@ifi.uzh.ch

Abstract

This article reports on the concept of electronic data safes for managing personal data and describes the landscape of existing services. Using an exploratory research approach, a model of hierarchical service layers is developed. It serves as a structure for orientation in this emerging field of tools and services. Furthermore, we identify factors and areas of interest that are relevant for the adoption of electronic data safes in e-government and e-business using the Unified Theory of Acceptance and Use of Technology as a theoretical lens. We conclude that clearly perceivable benefits are key facilitators for the adoption of electronic data safes by end-users.

1. Introduction

Personal data is managed in as manifold ways as there are types of personal data [39]. Many tools have been created to assist individuals in their data and (personal) information management – either paper based or electronically [17]. People connect more and more via social networks and provide personal data on a volunteered basis, or interaction as well as purchase data is tracked and collected by e-commerce companies. But tools supporting user-centric data management and providing users with means to execute informational self-determination to enforce privacy are still in their infancy and about to emerge [26]. We subsume all existing solutions and concepts under the umbrella term "electronic data safes". Such technological tools form part of a complex socio-technical system between individuals, service providers (public or private sector) and data safe providers.

Especially in the context of e-government and e-business service provision, these electronic data safes are expected to bring value to each user (individuals or organizations) [6]: For example, savings can be realized from optimized processes; data and documents can be exchanged that are accompanied by verified identity data, or transactions involving several (governmental) organizations will be facilitated. We argue, that electronic data safes will provide benefits to all user groups which could not be achieved if organizations stick to their information and process silos like organization-specific portals where users have to re-enter their personal data every time.

Two research questions are addressed: (1.) How can adequate structures be provided for discussing the emerging topic of electronic data safes? (2.) How can factors and areas of interest contributing to the adoption of electronic data safes be identified? In order to answer the first question, we will sharpen the concept of electronic data safes with a focus on e-government and e-business. As a result of our exploratory research, we (a) provide sensitizing concepts on how to talk about the emerging topic of electronic data safes and (b) present a model of hierarchical service layers which helps to give structure to the landscape of electronic data safe solutions. To answer the second research question, we attributed our model of hierarchical service layers with dimensions influenced by the Unified Theory of Acceptance and Use of Technology (UTAUT) [36] as a theoretical lens. Taking such a perspective, we are able to identify factors and areas of interest contributing to the adoption of electronic data safes.

2. Data Collection and Research Method

We followed an exploratory research approach, applying qualitative methods [27] such as literature analysis [24], guided interviews, and evaluation of existing data safe solutions as described in the following sections. We argue that using this triangulation approach [cf. 19] is an adequate way of data collection for emerging topics. First of all, the data sources we used are depicted. Then, we describe our sense-making approach that took place in order to create the model of hierarchical service layers and to identify factors for the adoption of electronic data safes.

2.1 Literature and Document Analysis

Domains, in which the concepts of electronic data safes emerge, were identified as: vendor relationship management (see section 4), cloud storage, and managing privacy for personal data. Furthermore, related areas were identified: electronic identity management systems (eIDMS), (personal) electronic health records management systems, electronic document delivery systems via digital postal services or e-billing and e-invoicing services. Additionally, a literature search using scientific literature databases (ACM, Scopus, IEEE, Citeseer, AISeL, GoogleScholar) as well as international union catalogues of library systems, and social bookmarking and citation sharing services was carried out. Literature specific to electronic data safes and the management of privacy with the help of technological tools was found to be very scarce. As an emerging topic that touches many related areas, there are some similar domains and concepts, but no unifying taxonomy exists which helps to give orientation. The following sources were used (numbers in brackets indicate the number of sources we have consulted), and, where possible, existing public (beta) services of electronic data safes (#7) or cloud storage services (#5) were accessed to gain hands-on experience. Publicly available descriptions, either self-issued by these service providers or written about them by other organizations were also included. These materials consisted mainly of: web pages (#55), journal articles (#52) white papers and reports (#49), research papers and studies (#42), press clippings (#23), blog entries (#13), books or dissertations (#13), other documents (#13) or publicly available annual reports (#2).

2.2 Analysis of Existing Data Safe Solutions

We analyzed the following existing electronic data safe solutions, either by gaining hands-on experience with public (beta) services or through the information provided on the web sites and/or personal interviews (see also next section). The following solutions were thoroughly examined: SecureSafe (Internet data safe solution, http://www.securesafe.com), (mein) Service-BW (portal of the state of Baden-Wuerttemberg in Germany for its citizens, http://www.service-bw.de), doMap (process-oriented portal of the city of Dortmund, Germany, http://www.domap.de), eBürgersafe (an application to demonstrate the usefulness of the electronic identity management system's functionality of the new German identity card, piloted in the state of Bremen and the city of Bremerhaven, Germany, http://www.buergersafe.bremen.de), Dokumentenablage (document safe) as part of the De-Mail portal in Germany (http://www.de-mail.de), e-Boks from Denmark (the Danish portal for electronic document delivery, http://www.e-boks.dk), and finally the Austrian E-Tresor (E-Safe, receiving documents supported by an eIDMS, http://www.e-tresor.at). Solutions related to digital document delivery and reception of electronic bills were analyzed focusing on Adminium (http://www.adminium.fr), Zumbox (http://www.zumbox.com), Doxo (http://www.doxo.com), Manilla (http://www.manilla.com) or Volly (http://www.volly.com). In the light of privacy managing tools, we analyzed the following solutions: Mydex (http://www.mydex.org), Pidder (http://www.pidder.com), Personal (http://www.personal.com), Azigo (http://www.azigo.com), TrustFabric (http://www.trustfabric.com), Qiy (http://www..qiy.nl), Singly (http://www.singly.com), and Allow (http://www.i-allow.com).

2.3 Qualitative Interviews

We further carried out seven interviews with stake-holders in the realm of electronic data safes each lasting about 90 minutes. The stakeholders were mainly representatives of organizations running an electronic data safe or people involved in designing such solutions, and academics doing research in this area. For all these interviews, a questionnaire had been prepared as a basis for each guided interview which was audio-recorded.

The design of the initial questionnaire was informed by literature on electronic data safes (notably [6]) as well as public accessible information on web pages or by testing existing data safe solutions. Consulting these sources, areas of interest emerged and were refined leading to a questionnaire with several categories. These categories were: a solution's context (stakeholders, history of the service, responsibilities for operating or developing the service, orientation on existing e-government strategies), design decisions concerning identity and access management, general functionalities of the service (for example, what data sharing mechanism are available), data on a solution's current usage (number of users, number of logins, etc.), its business model, and future directions. Each questionnaire was customized to every stakeholder and refined throughout the course of the data collection phase.

Additionally, two customers of an existing electronic data safe solution were interviewed to capture their views from a client's perspective. These interviews took about 45 minutes each. A questionnaire was used as a basis for the guided interviews. Questions were dealing with individual usage habits like

frequency, number of documents stored in their electronic data safe and their attitude towards security and the usability of their data safe's identity and access management from an end-user perspective.

2.4 Sense-making

The interview data was then summarized based on the structure of the questionnaires. To verify that nothing has been omitted, the individual reports were checked while re-listening to the audio-recordings. Finally, the reports were complemented with web findings and literature findings on the specific solution and an internal report documenting the state-of-the-art of electronic data safes has been compiled. During the composition of this report, a schema to organize the findings and to group data safe solutions emerged – in the tradition of exploratory research. We then generalized from this data and the model of hierarchical service layers (see section 6) was created which allowed us to sort data safe solutions according to their maturity and provided structure to the emerging landscape of electronic data safes thereby answering the first research question.

Based on this model of hierarchical service layers, we tried to answer the second research question: How to identify factors and areas of interest contributing to the adoption of electronic data safes? Therefore, we initially attributed our model of hierarchical service layers with dimensions influenced by the UTAUT as a theoretical lens. UTAUT was chosen because of its widespread use in information systems and its incorporation of prior technology acceptance models resulting in a parsimonious model with four constructs [36]: *Performance expectancy* is defined as "the degree to which an individual believes that using the system will help him or her to attain gains in job performance." *Effort expectancy* is defined as the "degree of ease associated with the use of the system." *Social influence* is defined as "the degree to which an individual perceives that important others believe he or she should use the new system." *Facilitating conditions* are defined as the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system." Further, UTAUT includes four moderating factors: *gender, age, experience,* and *voluntariness of use*.

The interview reports were analyzed for evidence of UTAUT's constructs and moderating factors. While working through the reports, we discovered that not all UTAUT constructs could be applied: No evidence was found for the constructs of social influence and all the moderating factors. During our sense-making process, we found evidence that other factors influencing the adoption exist:

We conclude that electronic data safes are network goods and they will benefit from network effects from both, the end-users, and the organizational users. UTAUT's "social influence" (oriented towards the end-users) can be subsumed under network effects, thereby also paying attention to the network effects which are clearly effective for all organizational users of electronic data safes. Furthermore, we included hedonics [16] as a dimension of analysis which originally is not included in the UTAUTs' constructs. Hedonic aspects originate from user-experience research in which the creation of a holistic user experience incorporating pragmatic qualities as well as hedonic qualities are regarded as necessary to design an appealing, interactive product. The pragmatic qualities help to achieve "do-goals", such as "making a telephone call" where functionalities and usability are decisive. In contrast, hedonic qualities support "be-goals" which give the reason why people are making a telephone call, such as the desire to relate to one's significant other [9].

3. What is "Personal Data"?

According to Kuneva [40], "Personal data is the new oil of the Internet and the new currency of the digital world." This citation illustrates the growing importance and value of personal data [38]. But what is personal data? We are taking a broader perspective informed by personal information management (PIM) and argue, that personal data are "information items" which are defined as packages of information that can be created, copied, stored, and retrieved etc. (e.g., digital photographs, music or references) [18]. We therefore classify personal information in five groups (based on [18,20,39]) forming a personal "information" ecosystem [cf. 39]: (1.) *Individual identity information items about me*: These information items officially identify an individual, for example, via the social security number. (2.) *Behavioral or observed information items:* All of these information items can be obtained through recording or observation while a customer uses a service, for instance, location data from mobile phones. (3.) *Derived or inferred information items:* This type of information items, such as the credit card score, is created by analyzing the behavioral data or voluntarily provided data. (4.) *Volunteered or self-identified information items sent or shared by myself:* Such information items are revealed by individual themselves. In social networks, for example, all group memberships, associations and "like"-comments as well as every piece of user-generated content forms part of this category. (5.) *Information items controlled by or owned by me*, which are, for example, photographs or music files.

This personal "information item" ecosystem is threatened by an imbalance between its three stakeholders: individuals, the public sector, and the private sector. If the private sector dominates, it is very likely that an almost uncontrolled data collection takes place which would deter end-users. If the public sector dominated with too rigid regulations, e.g. data protection laws, innovations and investments could slow down or even be prevented. This fairly new perspective on government as a beneficial regulator is about to evolve but in former times, government was regarded as being the "big brother" who wants keep his citizens under tight surveillance. If the end-users are let alone to self-regulation, islands of working solutions could establish (like Wikipedia) but much insecurity concerning the funding of services or the lack of governance could persist. Therefore, the ideal is to create a "win-win-win"-situation. [39]

Managing the personal information item ecosystem raises questions around privacy [29]. Internet users might use services on the web for free, but actually, they pay by providing personal information which can be aggregated to form profiles. In the sense of privacy, users should ideally know what information items they will exhibit and why. To enforce privacy, regulations as well as technological tools can be employed. Both will help individuals manage and control their personal information items, leading to a "New Deal on Data" [32] where informed consent is the key-mechanism [37]. Privacy-enhancing tools (e.g. offering encryption, digital pseudonyms or anonymous payment methods) and transparency-enhancing tools like Google's Dashboard (https://www.google.com/dashboard) to inform an individual which personal information items are stored and why, are helpful technologies in order to exert privacy [13]. In the next section, we will elaborate on electronic data safes as a socio-technical solution that helps individuals manage personal data.

4. Characterizing Electronic Data Safes

Since electronic data safes are an emerging topic, there are many parallel or slightly differing concepts used nowadays: (personal) data lockers, personal data stores, (personal) data vaults or, as we will call them, electronic data safes. They share some commonalities, either functions or concepts, but an established concept and term for this type of tools is lacking. In this paper, we follow the definition of [6] (translated by the authors of this paper): "An electronic data safe is a virtual data locker based on modern information and communication technologies which can be reached via electronic media in order to store, administer or share electronic data and documents." The owner (individuals, private or public sector organizations) of such an electronic data safe can share data on a fine-grained level with other parties.

If documents are transmitted entirely electronically, benefits from optimized processes with less manual errors due to changes in medium may be possible. Private sector organizations are also able to send data and documents to their customers via an electronic data safe [6]. Together with all (mobile) devices, such as smartphones or tablet PCs, a "personal cloud" [34] will evolve.

An electronic data safe is more than cloud storage as offered, for example, by Dropbox, Wuala, Windows Live SkyDrive, or Google Drive. Many of these offers do not provide encryption of the information stored (for a comparison of the security of cloud storage, see [5]) or a transfer of data to processes [35]. According [35], electronic data safes will provide benefits to all types of users because data and document delivery from trustworthy senders, data sharing mechanisms on a fine-grained level, and tight integration into business processes are combined in one place. For example, citizens will be able to share data from their electronic data safes with e-government processes and they can see and understand, in which parts of a process their data will be used.

In summary, these electronic data safes are tools to exert informational self-determination and to gain transparency on how information is used [2]. There are some fundamental requirements, electronic data safes have to fulfill [6]: (1.) guaranteed privacy that only the owner can access and share his or her data, (2.) an adequate technological, organizational and legal framework to protect the privacy of personal data, (3.) changing a service provider must not be complicated for end-users, (4.) if several data safes exist, they should be manageable under a single integrated user interface, (5.) sharing data and documents shall be supported by electronic identity management, and (6.) retention periods and service-level agreements must be obeyed and supported. Privacy-by-Design [8] will be essential in order to create trust in the service and its provider. The following section gives details on the history of electronic data safes.

5. History of Electronic Data Safes

In their position paper, Narayanan et al. [28] give a short historical background on the development of personal data stores, starting in the late 1990ies with "negotiated privacy techniques". Especially the concept of infomediaries (coined by [14]) was identified as a predecessor of today's personal data stores: "We believe that consumers are going to take ownership

of information about themselves and demand value in exchange for it." [14] But within five years after the concept of infomediaries has been around in the press or worked upon in scientific contexts, this whole movement as well as all commercial companies (Persona, Privada, Lumeria and AllAdvantage) vanished [28]. The idea of informational self-determination and receiving benefits and value in exchange for personal data continued in the "Project VRM" [33], which forms a conceptual counterpart of the traditional customer relationship management that was now reformulated as "vendor relationship management". With the help of VRM-tools like electronic data safes or personal data stores, customers should be able to emancipate from service providers and "bear their side of the relationship burden. […] Customers will be also be involved, as fully empowered participants, rather than as captive followers." [33]

Another predecessor for electronic data safes is the concept of a digital strongbox that was intended to support e-commerce processes and data and document exchanges [15].

We assume that creating transparency is a mechanism to increase trust. With respect to electronic data safes, this implies that a user must be able to understand where and which information items are used by whom. This relates to the need for process transparency [30] and information transparency. In the next section, a model for structuring the landscape of electronic data safes will be introduced.

6. Model of Hierarchical Service Layers

Narayanan et al. [28] offer a classification scheme for "personal data architectures". However, they suggested that other classifications might be possible as well. Based on our sense-making approach (see section 2.4), we argue that there are three hierarchically grouped service layers for electronic data safes: (1.) (cloud) storage services, (2.) value-added services, and (3.) process integration services. Every layer above can use the functionality provided by the layer below (see Figure 1).

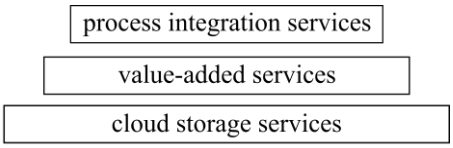

Figure 1: Hierarchical service layers

We assume that services provided by lower layers are reused on higher levels and that the higher layers will not have to re-implement them. If data safe solutions only work within one layer and are not using or providing functionalities to or from other layers, these electronic data safe solutions will face the need for re-adjusting or enlarging their functionalities and services in order to become successful, as explained later. Common to all service layers is their need for a high quality of service: On the one hand, this happens on a technological level (QoS) encompassing security, reliability, availability, etc. [4]. On the other hand, the entire service quality can be considered like completing an entire transaction on a web portal [31].

The foundational level is the *(cloud) storage layer* which encapsulates the basic services for storing data and providing data safety and security, e.g. by liberating the end-users to worry about backup procedures to be prepared against data loss. Moreover, access via several devices with possibly automatically transforming the information format of an information item according to the output device, synchronizing and backing up user data in a transparent, OS- and device-agnostic (smartphone, tablet, PC etc.) manner is performed on this service level.

The *value-added services layer* uses functionalities provided by the cloud storage layer. Additional services are offered providing value to the users. These services could be (non-conclusive enumeration): (a) sharing information items, e.g. like picture sharing or sharing thoughts and ideas like in social networks, (b) collaboration components, (c) automated report generation or data mining services on the information items sent to electronic data safes (e.g. Mint (http://www.mint.com) generates statistics on one's expenses), (d) vendor relationship management for exerting informational self-determination by providing mechanisms to manage one's privacy, e.g. like Mydex or Personal, and last but not least (e) data inheritance functionalities, e.g. to ensure that certain information items survive and are transferred or definitively destroyed if a user passes away, for example, as offered by the solution SecureSafe.

The last and topmost level is the *process integration services layer*. Building on the other two layers and their services, an electronic safe can be used to receive and deliver information items to e-government or e-business processes across organizations and is not tied to one (value-added) service provider. For instance, the SecureSafe solution is coupled with a Swiss bank's online banking portal so that the customers receive their electronic statements transmitted directly into the electronic data safe.

Our hierarchical service layer concept goes in line with the notion of vertically and horizontally integrated services with respect to personal information management [18] and the more radical suggestions of separating data storage and data use completely [3,21,25]: *Vertically integrated services* like Face-

book or YouTube are optimized to capture, store and disseminate specific information items under the realm of one single service provider. In contrast, *horizontally integrated services* would decouple the data storage and the value-added services, so that the features could be combined on demand and according to the user's preferences. Using our taxonomy of hierarchical service layers, we are able to group the existing and future electronic data safes solutions.

Cloud storage providers like Wuala or Dropbox nowadays are working mostly on layer one which is dealing with storage issues. Little value-added services are offered which prevents these services from being placed into the value-added layer.

On the second layer the *cluster of e-billing consolidators* is working: These services promise to ease the life of customers by fetching electronic bills from various providers (e.g. utility and telecommunication companies with their own portals) and to aggregate them at one place. Additional value is offered either by integrating payment and reminder functionalities or automated data-aggregation into statistics visualizing the personal expenses. In this category, many companies try to compete with each other as well as against many postal companies which are opening up new business opportunities [1]. Another cluster of applications working on layer two are the *account and inventory management services*: Solutions grouped into this cluster deal prominently with managing personal information items like account data or managing personal inventory, either locally on a single computer like InformationSafe (http://www.infosafe.com), or as a Software-as-a-Service like Reposito (http://www.reposito.com). The aforementioned service allows using multiple input devices such as PCs, smartphones or tablets to photograph items and to seize and store data – tasks that have to be facilitated by services provided by the (cloud) storage layer. A third cluster working on the level two of our proposed hierarchy of service layers are *personal data stores focusing on VRM*. These solutions adopted the VRM-paradigm that individuals should control their information items consciously and that they can decide and understand why and with whom they share them. Many of these services like Personal or Azigo have been launched in the last year and therefore they still are either in a (closed) beta testing or "opening soon" phase, like Mydex.

On level three (process integration services) there is one *cluster of solutions which were initially created or are still run by public service organizations and therefore have a deep rooting and inclination towards e-government.* Few of them offer value-added services like, for instance, Mydex that adopted the VRM paradigm and wants to offer integration into e-government processes. Recently, the concept of "Life Management Platforms" [23] was suggested combining the personal data store/VRM-vision with process integration of electronic data safes.

7. Identifying Factors for the Adoption of Electronic Data Safes

This section reports on the factors and areas of interest contributing to the adoption of electronic data safes. This is the result of an exploratory research approach whose method is described in section 2.4. Table 1 summarizes our findings by adding the main items of our discussion for each hierarchical service layer with respect to the corresponding dimension.

Cloud storage services: Effects of economy of scale are working on the network effects dimension and people are incentivized to use cloud storage solutions by the possibility of sharing content with others. They expect these cloud storage technologies to be as easily usable as any local storage component (relating to the dimension of effort expectancy). As a facilitating condition, the service provider's reputation and its terms and conditions are identified. E-Boks, although a privately owned company, is trusted which might be due to the shareholders that are trustworthy organizations per se: Post Danmark and Nets (payment and credit card processing services).

With cloud storage offerings, users expect data to be ubiquitously available, independent of the device used to access the data. Nevertheless, mechanisms to guarantee data security, safety, and privacy are established. As presented in the vision of electronic data safes, only the owner should be able to have access, neither the safe provider nor any other party without the owner's consent. This means, it has to be legally clarified if, at all, or under which circumstances and by which means the government should be granted access to an electronic data safe. This question reflects general security considerations and results in the following design requirements for electronic data safes: The data safe provider will not be able to have access to an individual's data therefore it is impossible to re-issue a "lost" private key which is used to individually encrypt users' data. Or, that every time data is accessed, this is logged for the transparency of the data owner. For example, the data safes of the Service-BW portal, Wuala or SecureSafe encrypt each data safe with a unique key managed only by the owner. These security services on the cloud storage layer should be available to the layers above.

Value-added services: Adding additional functionalities to the cloud storage layer generates additional value for the end-users. For example, services offer the collection of documents from different ser-

vice portals (utility providers, telecommunication companies) and create added-value by automatically generating reports on expenses based on the bills received, as performed by some of the e-billing consolidators like Adminium.

These functionalities give the users the means, that they can complete a certain task. For instance, managing their passwords and access data, obtaining financial overview or preventing paper clutter by going digital are all tasks touching the dimension of performance expectancy. Moreover, these services might provide ways to structure the information items received, for example, by offering folder structures, tagging mechanisms or full text retrieval – touching the dimension of effort expectancy. E-Boks in Denmark generates added value by helping users to organize their digital mail, for instance, by letting them create folders. Furthermore, information items can be shared with other users.

If the perceived benefits are judged positive, users might also be willing to share anonymously sensitive data. For instance, sharing health information items to allow anonymous data mining with the aim of detecting new insights and advancing science was a scenario an interviewee could imagine and continued: "Data collection and sharing are not bad per se – only what might be done wrong with it." This idea fits the dimension of network effects in relation to the value-added services: User may receive benefits through collaboration and data sharing, for instance using social bookmarking services. Or if they have agreed upon before, their anonymous data is used to collaborate "for them" with the help of data mining.

We also assume that "managing privacy" as proposed by [26] will be just one value-added service among others but users are far more attracted by service offerings helping them to achieve be-goals in respect to the hedonic dimension. Privacy itself will be regarded by the users as a hygiene factor which does not necessarily translate into a competitive advantage for a service provider because it will be expected to exist and work fine. This is also diagnosed in [11] and the authors of this study conclude that privacy will not "likely be a consumer driven issue, but rather an industry driven one".

Nevertheless, managing one's personal electronic identity (eID) will be certainly a necessity for using some of an electronic data safe's services and this will be judged within the dimension of effort expectancy. Research on eID-security shows [22] that the easier and more convenient authentication methods like software certificates or paper based transaction number lists are much more preferred to more complicated and safer authentication mechanisms. If services are created which show clear benefits of taking the pain of doing a more complex authorization, people will accept it. But if benefits are obscure, people will opt for the simpler solution. Existing eID management systems (eIDMS) on a national level should be successfully extended and expanded not only to serve the public sector, but also the private sector (dual use of a single authentication technology).

Table 1: summary of factors influencing the adoption of electronic data safes

Dimensions of observation / **Hierarchical service layers**	**Effort Expectancy**	**Performance Expectancy**	**Facilitating Conditions**	**Hedonic Aspects**	**Network Effects**
Process Integration Services	---	* integration of information items into processes * control an information item's usage * prevent media breaches	* legal context (receipt and acceptance of electronic documents) * standardization to provide interoperability	---	* very strong effects if private and public sector are participating
Value-Added Services	ease of use for: * structuring information items * electronic identity management system (dual use by private and public sector) * granting proper access rights	services must support goal-achievement: * password safes * financial overview by generated reports * inventory management * aggregation of bills and documents to prevent clutter	---	creating positive user experiences * using mobile devices which fit in the users' way of life * support the achievement of "be-goals"	provide collaboration mechanism: * share data voluntarily to collaborate * receive benefits via explicitly granted but anonymous data mining of personal data
Cloud Storage Services	* as easy as local storage	* ubiquitous access (place/device) * data security and safety	* reputation of the service provider * terms and conditions	---	* economies of scale * possibility of sharing content

For instance, the Austrian citizen card offers an eID-infrastructure based on a smart-card and authentication via mobile phones which potentially every Austrian citizen can use – but only a small number has actually activated this functionality. On the contrary, E-boks in Denmark uses the eID-infrastructure called NemID (easy ID) which has been widely accepted since its introduction in 2010 and which integrates the formerly separated solutions OCES (government-driven) and NetID (banks). This example shows that using convenient mechanisms and creating an infrastructure which can be used by private and public companies leads to a successful adoption. E-Boks acts as an intermediary between customers and organizations. But there might originate the risk that an intermediary might become obsolete because of the universal authentication infrastructure: Banks running existing e-banking solutions might argue that this easy login is convenient enough for their customers and therefore they want to avoid paying the intermediary for delivering documents the customer could get himself via the existing e-banking channels.

Data transparency is a double-edged sword. If people should be able to exert informational self-determination, controlling the use is one part of the activities. Granting the proper rights, which is assumed to take place more often in the context of electronic data safes, should require as little effort as possible, which touches the dimension of effort expectancy. Some authors argue, that from a cognitive perspective, users have to take an increasing number of decisions with whom they share data which possibly leads to cognitive overload [28].

Hedonic aspects are dealing with the joy of use. Services provided on the value-added layer therefore should provide a positive user experience. Reposito allows you to create an inventory as easily and joyfully as possible using smartphones. They are used as barcode scanners so that a user can forget about typing in product data and it assists in documenting an inventory item and integrating all information in one place. In such a way, hedonic aspects of "be-goals" like documenting one's inventory for the case of accidents overcomes the status of being a cumbersome "do-goal" activity.

Process integration services: On the layer of process integration services, network effects will have strong influences: The more processes are offered, the more users are attracted. E-Boks has 20'000 senders from the private and public sector and it has 5.3 million users [10].

The vision of electronic data safes [6] suggests that benefits can be achieved if individuals share information items with processes. For example, account or salary statements could be transmitted electronically to the tax office – without having to switch media. This relates to the dimension performance expectancy. Such integration on the process level stimulates the performance expectation, that users can purposefully use an electronic data safe to achieve goals and keep track where their data is used.

Providing interoperable process chains surmounting organizational boundaries will be a key challenge for the adoption of electronic data safes. People are weary of re-entering the same data on different web sites to accomplish a task [7]. If data can be re-used across organizations or across several government agencies, electronic data safe users experience substantial benefits. But as a precondition, technical, semantic, organizational, and legal interoperability [12] must be established. Electronic data safes benefit from standardization initiatives as facilitating conditions.

Storing data online per se has its benefits (as seen in the success of cloud based storage: being able to access or synchronize data from multiple places with multiple devices), but electronic data safes will certainly not be attractive for users when no other benefit is offered. Existing service offerings of electronic data safes with no process integration (for instance, the e-Bürgersafe in Bremen) are actually used far below the expectations of the service providers, as one interviewee stated.

If electronic data safes are able to receive documents or data with legally binding content (e.g. contracts) or documents associated with an objection period, current work practices and processes needs to be supported with electronic data safes in an analogous way – which is a facilitating condition. For instance, if a postal company sends a registered letter in order to document the reception on behalf of the sender, the organizational, legal, and technological tools should be able to offer the same services digitally. From a legal point of view, it should be clear what the consequences of a failed reception are (for example while being on holidays) or if transfer errors occur. In Austria, this has been legally clarified in the Service of Documents Act.

Another factor which will have influence on the facilitating conditions was identified in the legal acceptance of electronic documents. Many laws, e.g. for taxation, require documents to fulfill certain qualities – being original, unaltered and with approved origin. These "paper-world" concepts were transformed into requirements for handling digital documents, adding a lot of complexity like a forced usage of (qualified) digital signatures. Sticking to such rigid mappings of the paper world to the digital world will impose big barriers for the adoption. Rethinking laws and providing "reasonable" and "moderate" ways of

handling digital data and documents in a legally conform way will be key facilitators for the adoption of electronic data safes. Using functionalities from lower layers, services can be created or re-designed so that, for example, documents can be "scanned" using a smartphone and delivered to a business process.

8. Discussion and Conclusion

With the help of our model of hierarchical service layers that we attributed with dimensions from UTAUT and adding the dimensions of network effects and hedonic aspects, we could gain insights in the current landscape of electronic data safes. This approach allowed us to identify factors and areas of interest which might serve as facilitators or barriers for the adoption of electronic data safes. We assume that the model of hierarchical service layers is so generic that it can be applied in other context where there is a need for decoupling data management and data processing for service provision.

Our sense-making approach was performed in an exploratory stage of research and our findings needs to be validated – ideally by integrating experiences of real users of electronic data safe solutions. So far, only two end-users of electronic data safe solutions have been interviewed. Further research should focus on (potential) end-users and their expectations of electronic data safes. By contrasting their expectations with the current landscape of electronic data safes, design principles could be questioned, refined or newly discovered. The dimensions taken from the UTAUT were considered to be quite helpful during the sense-making process. Further research is necessary to explain why some constructs on certain hierarchical service levels could not be supported by data and what this implies for the selected dimensions.

If data safe solutions work exclusively on one hierarchical service layer and do not integrate the previous ones, they will become vertically integrated solutions or islands where potential benefits for customers might be hard to achieve: For example, this happens if an electronic data safe does not have any data sharing capabilities or data cannot be transferred to processes. Therefore, it is necessary that services will use functionalities provided from lower levels of our model of hierarchical service layers. For instance, services can be created or re-designed so that documents can be "scanned" using a smartphone and later on delivered to a business process, which is provided as functionality on a higher level.

To synthesize our findings, we conclude that clearly perceivable benefits are the key facilitators for the adoption of electronic data safes arising from the UTAUT dimensions of performance and effort expectancy. As implications for practice, we suggest that electronic data safe solutions should put emphasis on their ease of use. Furthermore, value-added services should be developed that appeal to hedonic aspects but at the same time contribute to users' demands originating from the dimension of performance and effort expectancy. All these value-added services should be able, if necessary, to be integrated into business processes in order that users can achieve "be-goals" and not only "do-goals".

9. References

[1] accenture. *Achieving High Performance in the Postal Industry*. 2011.

[2] Andrieu, J. *The Information Sharing Report*. Kantara Initiative, 2010.

[3] Ates, M., Ravet, S., Ahmat, A.M., and Fayolle, J. An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights. *Sixth International Conference on Availability, Reliability and Security (ARES)*, IEEE (2011), 555–560.

[4] Badger, M.L., Grance, T., Patt-Corner, R., and Voas, J.M. *Cloud Computing Synopsis and Recommendations*. 2012.

[5] Borgmann, M., Hahn, T., Herfert, M., et al. *On the Security of Cloud Storage Services*. 2012.

[6] Breitenstrom, C., Brunzel, M., and Klessmann, J. *Elektronische Safes für Daten und Dokumente*. Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS), Berlin, 2008.

[7] Brustein, J. Start-Ups Aim to Help Users Put a Price on Their Personal Data. *NYTimes.com*, 2012, B3. http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[8] Cavoukian, A. *Privacy by Design... take the Challenge*. Information and Privacy Commissioner of Ontario Canada, Ontario, Canada, 2009.

[9] Diefenbach, S. and Hassenzahl, M. The dilemma of the hedonic – Appreciated, but hard to justify. *Interacting with Computers 23*, 5 (2011), 461–472.

[10] e-Boks. *E-Boks Årsrapport 2010*. 2011.

[11] Ericsson. *Consumer Privacy in an Online World. An Ericsson Consumer Insight Summary Report*. Ericsson, Stockholm, 2012.

[12] European Commission. Towards interoperability for European public services. COM(2010) 744 final. 2010.

[13] Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., and Waidner, M. *Online Privacy: Towards Information Self-Determination on the Internet*. Dagstuhl Workshop, Dagstuhl, 2011.

[14] Hagel III, J. and Rayport, J.F. The Coming Battle for Customer Information. *Harvard Business Review*, January-February Reprint Number (1997), 5–11.

[15] Hardjono, T. and Seberry, J. Design and security issues in strongbox systems for the internet. *Faculty of Informatics - Papers*, (1996).

[16] Hassenzahl, M. Experience Design: Technology for All the Right Reasons. *Synthesis Lectures on Human-Centered Informatics 3*, 1 (2010), 1–95.

[17] Jones, W. and Teevan, J., eds. *Personal Information Management*. Univ of Washington Pr, 2007.

[18] Jones, W. *The Future of Personal Information Management, Part I: Our Information, Always and Forever*. Morgan & Claypool Publishers, 2012.

[19] Kaplan, B. and Maxwell, J. Qualitative research methods for evaluating computer information systems. *Evaluating the Organizational Impact of Healthcare Information Systems*, (2005), 30–55.

[20] Khatibloo, F. *Personal identity management*. Forrester Research, 2011.

[21] Van Kleek, M., Smith, D., Shadbolt, N., and others. A decentralized architecture for consolidating personal information ecosystems: The WebBox. (2012).

[22] Kubicek, H. and Noack, T. *Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich*. LIT, Münster, 2010.

[23] Kuppinger, M. *Advisory Note: Life Management Platforms: Control and Privacy for Personal Data*. 2012.

[24] Levy, Y. and Ellis, T.J. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline 9*, (2006), 181–212.

[25] Mun, M., Hao, S., Mishra, N., et al. Personal data vaults: a locus of control for personal data streams. *Proceedings of the 6th International Conference*, ACM (2010), 17:1–17:12.

[26] Mydex. *The Case for Personal Information Empowerment - The rise of the personal data store.* Mydex, 2009.

[27] Myers, M.D. Qualitative Research in Information Systems. *MIS Quarterly 21*, 2 (1997), 241.

[28] Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., and Boneh, D. A Critical Look at Decentralized Personal Data Architectures. *arXiv:1202.4503*, (2012).

[29] Nissenbaum, H.F. *Privacy in context : technology, policy, and the integrity of social life*. Stanford Law Books, Stanford, Calif., 2010.

[30] Nussbaumer, P. and Matter, I. What You See Is What You (Can) Get? Designing for Process Transparency in Financial Advisory Encounters. *Human-Computer Interaction – INTERACT 2011*, Springer Berlin Heidelberg (2011), 277–294.

[31] Papadomichelaki, X., Magoutas, B., Halaris, C., Apostolou, D., and Mentzas, G. A review of quality dimensions in e-government services. *Proceedings of the 5th international conference on Electronic Government*, Springer-Verlag (2006), 128–138.

[32] Pentland, A. Reality mining of mobile communications: Toward a new deal on data. *The Global Information Technology Report 2008–2009*, (2009), 1981.

[33] Project VRM. Main Page - Project VRM. 2012. http://cyber.law.harvard.edu/projectvrm/Main_Page.

[34] Reed, D., Johnston, J., and David, S. *The Personal Network: A New Trust Model and Business Model for Personal Data*. Connect.Me, 2011.

[35] Schulz, S., Hoffmann, C., Klessmann, J., Penski, A., and Warnecke, T. *Dienste auf Basis elektronischer Safes für Daten und Dokumente*. Lorenz-von-Stein-Institut, Fraunhofer FOKUS, 2010.

[36] Venkatesh, V., Morris, M.G., Gordon B. Davis, and Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly 27*, 3 (2003), 425–478.

[37] Whitley, Edgar A. Informational privacy, consent and the "control" of personal data. *Information Security Technical Report 14*, 3 (2009), 154–159.

[38] World Economic Forum, W. *Rethinking Personal Data: Strenghtening Trust*. World Economic Forum, 2012.

[39] World Economic Forum. *Personal Data: The Emergence of a New Assest Class*. 2011.

[40] EUROPA - Press Releases - Meglena Kuneva, European Consumer Commissioner, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling , Brussels, 31 March 2009.